

Anonymous broadcasting with a continuous-variable topological quantum code

Nicolas C. Menicucci,¹ Tommaso F. Demarie,^{2,3} and Gavin K. Brennen³

¹*School of Physics, The University of Sydney, Sydney, NSW 2006, Australia*

²*Singapore University of Technology and Design, 20 Dover Drive, Singapore 138682*

³*Centre for Engineered Quantum Systems, Department of Physics and Astronomy, Macquarie University, North Ryde, NSW 2109, Australia*

(Dated: March 4, 2015)

Broadcasting information anonymously becomes more difficult as surveillance technology improves, but remarkably, quantum protocols exist that enable provably traceless broadcasting. The difficulty is making scalable entangled resource states that are robust to errors. We propose an anonymous broadcasting protocol that uses a continuous-variable toric-code state, which can be produced using current technology. High squeezing enables large transmission bandwidth and strong anonymity, and the topological nature of the state enables local error correction.

Introduction.—Almost every aspect of modern society relies on information processing. As digital surveillance capabilities continue to expand [1], so does demand for guaranteed-anonymous communication strategies. An example of such protocols is anonymous broadcasting, an important primitive for privacy-preserving routines [2]. Repeated use of such schemes could enable, for example, tipping off the police anonymously, secret balloting, and secure electronic auctions [3]. In the original classical formulation [4], and its improvements [5, 6], n parties establish shared keys enabling one party to reveal one bit of information while keeping her identity secret. The first *quantum* protocol that allows one to communicate classical information anonymously was proposed in [7]. A more efficient and secure quantum protocol for anonymous quantum and classical broadcasting was reported by Christandl and Wehner in [8]. Here, a trusted resource distributes ahead of time an n -partite entangled state $|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|0_1 \cdots 0_n\rangle + |1_1 \cdots 1_n\rangle)$, one qubit to each party. The key feature of this quantum protocol is that it is completely *traceless*—i.e., the sender’s identity cannot be determined (better than guessing) even if all resources are made public at the end of the protocol. Remarkably, tracelessness cannot be achieved classically.

Both the protocol in [8] and its later improvements [9, 10], however, suffer from decoherence from unwanted interactions with the environment. Indeed, the issue of decoherence is rather challenging to overcome, and it has surprisingly been ignored in all previous works.

A solution to this problem is to encode the resource in a quantum error-correcting code [11]. Such a code should be fast to prepare in practical settings and should be easy to error correct using mostly local operations by the parties involved. Here we present a protocol for quantum-assisted anonymous broadcasting using a recently developed continuous-variable (CV) toric code [12]. Surface codes have been extensively studied for the purpose of providing sustained quantum memories or for fault-tolerant quantum computation [13], and recent experiments [14] have built small prototype qubit toric codes. However, the overhead in gates and qubits for such quantum processing is daunting [15]. Our work shows that

much simpler tasks for communicating *classical information* benefit from the topological protection of such codes, and the CV model is an ideal candidate since it can be quickly prepared and distributed to the parties and it provides large communication bandwidth limited only by the squeezing level.

We first introduce the main idea using the discrete-variable (DV) toric code, and then generalize the discussion to its CV analogue. In fact, while such a state offers natural resilience against errors, it also allows for a larger bit rate than either the classical or the discrete quantum counterpart. Furthermore, it can be easily prepared using Gaussian resources and operations, and we describe experimental implementations that could be implemented with current technology.

DV toric-code anonymous broadcasting.—We illustrate the main idea with a qubit toric code. Consider a two-dimensional square lattice on a torus with qubits on the edges. The code states are $+1$ eigenstates of all stabilizers, $\hat{A}_v = \prod_{+v} \hat{X}_e$ and $\hat{B}_f = \prod_{\square_f} \hat{Z}_e$, defined at all vertices v and all faces f of the lattice, respectively [16, 17]. On the torus there are four such stabilizer states $\{|\text{GS}_{ab}\rangle = X_{\vec{p}_1}^a \otimes X_{\vec{p}_2}^b |\text{GS}_{00}\rangle\}_{a,b \in \{0,1\}}$ encoding two logical qubits [18]. The logical operators are string operators: $\hat{Z}_{\mathcal{P}_j} = \prod_{e \in \mathcal{P}_j} \hat{Z}_e$ and $\hat{X}_{\vec{\mathcal{P}}_j} = \prod_{e \in \vec{\mathcal{P}}_j} \hat{X}_e$, where \mathcal{P}_j and $\vec{\mathcal{P}}_j$ are loops on the lattice and dual lattice, threading through or around the hole in the torus (see Fig. 1).

Here and in the following we always consider a scenario with n participants, of whom exactly one of them, Alice, wants to anonymously broadcast a public message. The anonymous broadcast protocol works by preparing the fiducial state $|\text{GS}_{00}\rangle = \prod_v \frac{1}{\sqrt{2}}(\hat{I} + \hat{A}_v)|0 \cdots 0\rangle$ and distributing n wedges of the torus, one to each party (see Fig. 1). When Alice wants to anonymously broadcast the message $r = 1$ she performs the string operation $\hat{X}_{\vec{\mathcal{P}}_2}$ around the loop on her wedge [see Fig. 1(c)], while for the message $r = 0$ she does nothing. Next, each party j measures qubits in the \hat{Z} basis along an arc of the wedge, and publicly announces the parity m_j of $+1$ outcomes. The broadcast message is recovered from the sum $\sum_{j=1}^n m_j = r \pmod{2}$. When using a graph with

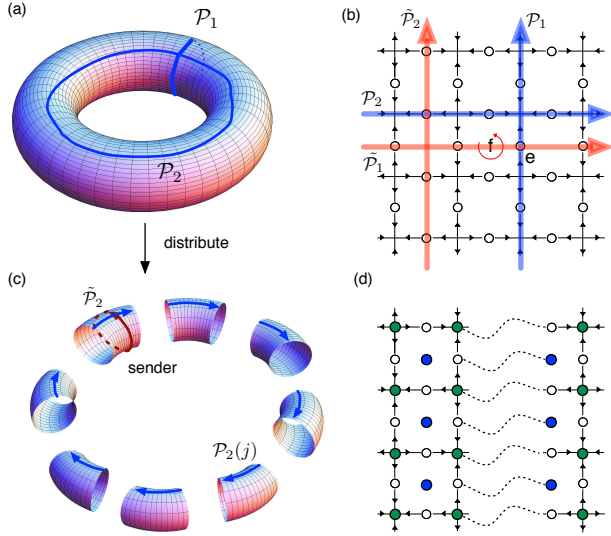


FIG. 1: Sketch of the protocol. (a) A CV toric code is prepared in the ground state of the two non-local string modes where the relevant loops are shown in blue. (b) Close-up of the lattice. Physical bosonic modes are logically assigned to each edge, and each edge is assigned an orientation. Similarly, the faces are given a uniform orientation. For the indicated face and edge, $o(e, f) = +1$ and $f(e) = -1$ with respect to path $\tilde{\mathcal{P}}_1$ and $o(e) = +1$ with respect to path \mathcal{P}_1 (see main text). (c) The state is distributed to n parties, one wedge to each. A sender Alice performs the unitary operator $\exp[i|\mathcal{P}_2|^{1/2} r \sum_{e \in \tilde{\mathcal{P}}_2} f(e) \hat{q}_e]$ on a loop (shown in red) around her wedge, which encodes a message $r \in \mathbb{R}$. Next, each party j measures an operator $\hat{M}_j := |\mathcal{P}_2(j)|^{-1/2} \sum_{e \in \mathcal{P}_2(j)} o(e) \hat{p}_e$ along an arc $\mathcal{P}_2(j)$ of the loop \mathcal{P}_2 (shown in blue). The parties then publicly announce their measurement outcomes $\{m_j\}_{j=1}^n$, and the broadcast message is computed as their (noisy) weighted sum. (d) Close-up of the error mitigation strategy. The blue (green) ancillas are coupled to modes surrounding faces (vertices) and are monitored for decay to prevent errors using the quantum Zeno effect. Couplings across boundaries between wedges are enabled via long range bosonic channels (dotted lines).

$|\tilde{\mathcal{P}}_2| = 1$ (i.e., just one qubit wide, a loop along \mathcal{P}_2), then $|\text{GS}_{00}\rangle$ is just a GHZ state in the $|\pm\rangle$ basis. For such a torus (loop), $\tilde{\mathcal{P}}_1$ and \mathcal{P}_1 are undefined, vertex stabilizers reduce to pairs of adjacent Paulis ($\hat{X}\hat{X}$) along $\tilde{\mathcal{P}}_2$, and face stabilizers do not exist. In either case (GHZ or full toric code), the variance of any individual party's measurement is maximal, and no collusion by any proper subset of the non-broadcasting parties will reveal any information about the identity of the broadcaster. Using a qudit toric code [19] (or qudit GHZ state) the protocol generalizes to give $\sum_{j=1}^n m_j = \#\text{broadcasters} \pmod{d}$, thus allowing up to $d-1$ broadcasters. Alternatively, by applying the string operator $X_{\tilde{\mathcal{P}}_2}^r$ for $r \in \mathbb{Z}_d$, a single party can anonymously broadcast $\log_2 d$ bits per round.

The advantage of using a toric code state instead of a simple GHZ state appears when one considers noise (er-

rors) in the protocol. Notably, since errors in the surface code can be diagnosed by measuring stabilizers, all such measurements and corrections are local to each party—except for those stabilizers that straddle the boundary between wedges [see Fig. 1(d)]—and can be corrected without disrupting the protocol [20, 21]. The non-local stabilizers could be measured with the assistance of Bell pairs shared between nearest-neighbor parties to enable non-local gates [22]. Then, the number of entangled pairs needed grows as the number of parties and the size of the wedges—which, we show below, is a small constant.

CV toric code anonymous broadcasting.—The ideal CV surface code [23] is a straightforward generalization of the qudit surface code, but it represents an unphysical model because the required states are infinitely squeezed. The finitely squeezed CV surface code is an experimentally accessible, physical approximation of this code [12]. This model starts with an $n \times m$ square lattice endowed with oriented edges $\{e\}$ and faces $\{f\}$, just like in the qudit case [12, 19]. An independent bosonic mode is logically assigned to each edge of the lattice, with quadrature operators \hat{q}_e, \hat{p}_e obeying $[\hat{q}_e, \hat{p}_{e'}] = i\delta_{e,e'}$ (having set $\hbar = 1$). The CV surface-code state is defined as the state annihilated by the set of vertex nullifiers $\{\hat{a}_v = \frac{1}{\sqrt{8}} \sum_+ (s\hat{q}_e + is^{-1}\hat{p}_e)\}$ and face nullifiers $\{\hat{b}_f = \frac{1}{\sqrt{8}} \sum_{\square} o(e, f) (s\hat{p}_e - is^{-1}\hat{q}_e)\}$, where s is the local mode-wise squeezing factor, and the orientation sign factor $o(e, f) = \pm 1$ if edge e is oriented the same (opposite) as face f . Note that $[\hat{a}_v, \hat{a}_{v'}] = [\hat{b}_f, \hat{b}_{f'}] = [\hat{a}_v, \hat{b}_f] = [\hat{a}_v, \hat{b}_f^\dagger] = 0$; however, $[\hat{a}_v, \hat{a}_v^\dagger] \neq 0$ and $[\hat{b}_f, \hat{b}_f^\dagger] \neq 0$. A CV surface-code state $|\text{GS}\rangle$ satisfies $\hat{a}_v|\text{GS}\rangle = \hat{b}_f|\text{GS}\rangle = 0 \quad \forall v, f$.

On the torus, for the case with n and m even, there are only $n-1$ independent vertex and $m-1$ independent face nullifiers. Hence the nullifiers do not span the space of physical modes, and analogously to the two qubits encoded in the qubit toric code [13], there are two unconstrained *string modes* in the CV toric code. Defining two oriented paths \mathcal{P}_1 and \mathcal{P}_2 along the non-contractable loops of the torus [see Fig. 1(a-b)], the annihilation operators for the two string modes are

$$\hat{f}_j := \sum_{e \in \mathcal{P}_j} \frac{o(e)}{\sqrt{2|\mathcal{P}_j|}} (s\hat{p}_e - is^{-1}\hat{q}_e), \quad (1)$$

for $j = 1, 2$, where $|\mathcal{P}_j|$ is the loop length and $o(e) = \pm 1$ if edge e is oriented in the same (opposite) direction as \mathcal{P}_j . These operators satisfy the canonical commutation relations. Since each string touches an even number of modes of each nullifier with opposite signs due to edge orientations, we have by construction: $[\hat{f}_j, \hat{a}_v] = [\hat{f}_j, \hat{a}_v^\dagger] = [\hat{f}_j, \hat{b}_f] = 0$. Note that $[\hat{f}_j, \hat{b}_f^\dagger] \neq 0$. For the broadcasting protocol, we will make use of the non-local string momentum operator

$$\hat{M} := \frac{1}{\sqrt{|\mathcal{P}_2|}} \sum_{e \in \mathcal{P}_2} o(e) \hat{p}_e = \frac{1}{s} \frac{(\hat{f}_2 + \hat{f}_2^\dagger)}{\sqrt{2}}. \quad (2)$$

In the limit $s \rightarrow \infty$ [24], \hat{M} remains well defined even while the \hat{f}_j do not. Intuitively, the CV surface-code state can be prepared by performing appropriate measurements on a CV cluster state [24], as described in Ref. [12]. The prepared encoded state is a displaced ground state of the string modes (see Section I in the Supplement). The displacement can be completely accounted for by subtracting it from the broadcast message, and therefore we assume $\hat{f}_1|\text{GS}\rangle = \hat{f}_2|\text{GS}\rangle = 0$.

The protocol with finite squeezing.—The protocol is summarized in Fig. 1. The finitely squeezed CV toric-code state is prepared with the string modes in the ground state. The variance of the string momentum operator \hat{M} is $(\Delta M)^2 = \frac{1}{2s^2}$, with $\langle \hat{M} \rangle = 0$ (see Section II in the Supplement). The code state is distributed, one wedge to each party. Assume Alice wishes to anonymously broadcast the real number r . This means displacing the string momentum $\hat{M} \mapsto \hat{M} + r$ by means that are not detectable once the measurements have begun [8]. To this end, she performs the unitary $\exp[i|\mathcal{P}_2|^{1/2} r \sum_{e \in \tilde{\mathcal{P}}_2} f(e)\hat{q}_e]$ along a loop $\tilde{\mathcal{P}}_2$ of her wedge. Here $f(e) = \pm 1$ if the edge e has the same (opposite) direction as the framing of the path $\tilde{\mathcal{P}}$, where the framing of a path is to the right and normal to its direction [see Fig. 1(b)]. Then, each party holding wedge j measures the Hermitian operator $\hat{M}_j := |\mathcal{P}_2(j)|^{-1/2} \sum_{e \in \mathcal{P}_2(j)} o(e)\hat{p}_e$ along an arc $\mathcal{P}_2(j)$ of the loop \mathcal{P}_2 with outcome $m_j \in \mathbb{R}$. Note that $\mathcal{P}_2 = \bigcup_{j=1}^n \mathcal{P}_2(j)$ must be a closed loop. This implies pre-agreement between the parties and active communication during the protocol to establish a different connected path in case of errors at the end points. After the measurements, all parties publicly announce their results $\{m_j\}$, and using $\langle \hat{M} \rangle = 0$ the transmitted message from Alice can then be inferred from the (noisy) weighted sum $M = |\mathcal{P}_2|^{-1/2} \sum_{j=1}^n |\mathcal{P}_2(j)|^{1/2} m_j$, which is equivalent to measuring \hat{M} , which (after the broadcast) has mean r and variance $(\Delta M)^2 = \frac{1}{2s^2}$ [63].

Anonymity and channel capacity.—Finite squeezing means the broadcast will not be completely anonymous. Anonymity is predicated on the assumed inability to identify the broadcaster based on the local measurement outcomes. The degree to which this is true depends on signal-to-noise ratio (SNR) of the message strength to the noise in the local measurement. We want this to be small for high anonymity. But the signal strength cannot be too small lest the broadcast be too weak to be detected.

The variance of each local measurement $(\Delta M_j)^2 = \frac{1}{2s^2} + \frac{s^2}{w}$ is dictated by the \hat{p} - \hat{p} correlations, which are computed in [12] (see Section II in the Supplement for details). Here, $w = |\mathcal{P}_2(j)|$ is the width of the wedge held by each party (henceforth assumed equal). Remember that the global measurement outcome M has variance $(\Delta M)^2 = \frac{1}{2s^2}$. Here we quantify the amount of information an eavesdropper can obtain about the sender's identity A from the measurement

record \mathbf{M} , assuming that only one sender (Alice) will send a message r , chosen from a Gaussian-distributed random variable R with mean 0 and variance τ^2 . We also assume, a priori, that we have no information about the identity of the sender.

To quantify the loss of anonymity, we model this as (unintentional) classical communication of the sender's identity A through a channel whose output is the measurement record \mathbf{M} . Therefore, the quantity of interest is the mutual information $I(\mathbf{M}; A)$ between \mathbf{M} and A . We find explicitly the upper bound (see Section IV in the Supplement)

$$I(\mathbf{M}; A) \leq \frac{1}{2} \log \left[\frac{T_n(1 + \epsilon + \epsilon\alpha) - 1}{(1 + \epsilon\alpha \frac{\partial}{\partial \epsilon})(T_n(1 + \epsilon) - 1)} \right], \quad (3)$$

where $T_n(x)$ is the n th-order Chebyshev polynomial of the first kind, and the base of the logarithm determines the information unit (base 2 \rightarrow bits, $e \rightarrow$ nats, 10 \rightarrow digits, etc.). Here we have defined

$$\epsilon := \frac{(\Delta M)^2}{(\Delta M_j)^2 - (\Delta M)^2}, \quad \alpha := \frac{\tau^2}{(\Delta M)^2}. \quad (4)$$

$\epsilon = \frac{w}{2s^4}$ quantifies the ratio of global noise to additional local noise in the resource state, with $\epsilon \ll 1$ for a good resource (large squeezing), and $\alpha = 2s^2\tau^2$ is the SNR of the broadcast message [64]. The remaining amount of uncertainty about the sender's identity A after knowing the measurement record \mathbf{M} is the conditional entropy $H(A|\mathbf{M}) = H(A) - I(\mathbf{M}; A) = \log n - I(\mathbf{M}; A)$. Expressing this in bits (log base 2), the probability to detect the sender given the measurement record is then $2^{-H(A|\mathbf{M})}$. For good resource states, we can expand $I(\mathbf{M}; A)$ to $O(\epsilon)$ (see Section IV in the Supplement) and show that $\epsilon\alpha \ll 6$ guarantees high anonymity due to Alice's broadcast being hidden by the noise of the local measurements.

The broadcast channel is an unbiased Gaussian channel that adds noise with variance $\frac{1}{2s^2}$ to the message R . The mutual information $I(R; M)$ between R and the output message M is therefore a simple function of the broadcast's SNR α . It can be shown (see Section III in the Supplement) that, conditioned on a fixed signal variance τ^2 , a Gaussian-distributed message R maximizes this mutual information. Thus, the (variance-restricted) broadcast channel capacity as a function of the SNR is equal to this mutual information:

$$C(\alpha) = I(R; M) = \frac{1}{2} \log(1 + \alpha). \quad (5)$$

Clearly, then, there is a tradeoff between anonymity and channel capacity [65] (see Fig. 2).

Error mitigation.—To be robust to decoherence, we need a way to mitigate errors on the CV surface code. We assume errors are local and occur with a uniform rate γ_{err} for all modes. A local mode error takes the code outside the nullspace of some or all of the nullifiers touching that mode and may include photon loss or a more general

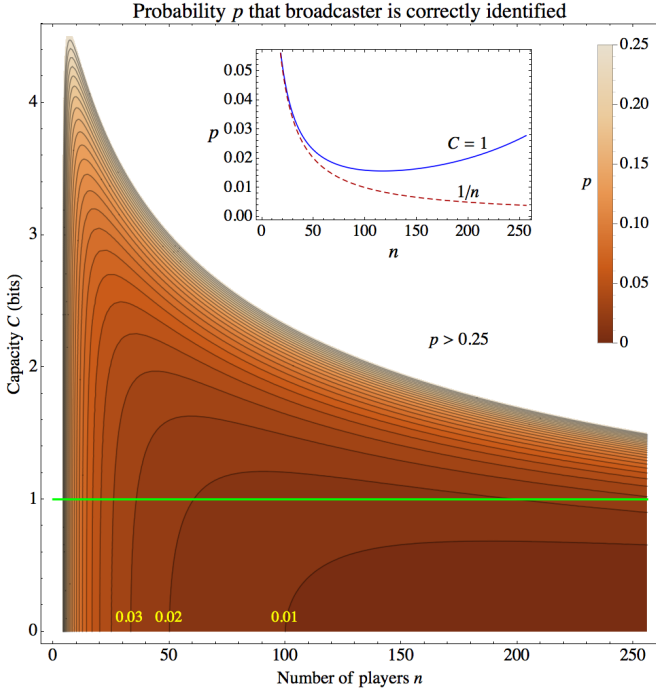


FIG. 2: Contour plot of the maximum probability p the broadcaster is correctly identified during the protocol as a function of the number of players n and the channel capacity C [Eq. (5)]. Contours corresponding to $p = 0.01, 0.02, 0.03$ are labeled, and subsequent contours increase by 0.01 each. The white region corresponds to $p > 0.25$. The squeezing is 20 dB ($s = 10^{(\#dB)/20} = 10$), and each player's wedge width is $w = 6$ (see Section V in the Supplement). The inset shows (i) a solid blue curve corresponding to a cross section of the main plot along the green $C = 1$ line and (ii) a dashed red curve corresponding to $p = 1/n$. The latter corresponds to perfect tracelessness (no more risk than guessing randomly), which is only achieved in the trivial limit of no broadcast ($C = 0$) or, for any $C > 0$, in the asymptotic limit of infinite squeezing.

local error. Our error-avoidance strategy is to continually drive the CV surface code back into the null space of its local nullifiers $\{\hat{a}_v, \hat{b}_f\}$ by reservoir engineering. This is done by embedding ancillary modes $\{\hat{c}_v\}$ and $\{\hat{d}_f\}$ at each vertex and face of the lattice respectively and using interaction sequences with the system followed by ancillary mode decay. A suitable interaction between the code state and the ancilla is the quadratic Hamiltonian $\hat{H}_{\text{int}} = g[\sum_v (\hat{c}_v^\dagger \hat{a}_v + \hat{c}_v \hat{a}_v^\dagger) + \sum_f (\hat{d}_f^\dagger \hat{b}_f + \hat{d}_f \hat{b}_f^\dagger)]$. Meanwhile the ancillary modes are subject to local decay with this map on the state $\hat{\rho}$: $\hat{\mathcal{L}}_a = \sum_v \hat{\mathcal{L}}_v + \sum_f \hat{\mathcal{L}}_f$ where $\hat{\mathcal{L}}_v[\hat{\rho}] = -\delta(\hat{c}_v^\dagger \hat{c}_v \hat{\rho} + \hat{\rho} \hat{c}_v^\dagger \hat{c}_v)$ and $\hat{\mathcal{L}}_f[\hat{\rho}] = -\delta(\hat{d}_f^\dagger \hat{d}_f \hat{\rho} + \hat{\rho} \hat{d}_f^\dagger \hat{d}_f)$ [66]. These coherent and incoherent interactions would be left on for the duration of the protocol so that errors are inhibited from occurring by the quantum Zeno effect [25–27]. Monitoring the environment near the ancillary modes for decay, the system can be realistically projected into the desired code state provided we are in the “good” measurement regime defined by the condi-

tion [25]: $g \ll \delta \ll g^2/\gamma_{\text{err}}$. The left inequality requires that the amount of population in the decaying ancillary modes is very small (so that decay events are rare), while the right inequality guarantees that the measurement of decay from the ancillary modes is sufficiently strong to damp coherences between code and faulty states on the time scale they are induced due to errors. When an error is detected, the players can deform their paths around this error as long as the wedges are large enough (see Section V of the Supplement).

Implementations.—This protocol may be implemented using recently demonstrated methods for generating large-scale optical CV cluster states encoded in either frequency modes [28, 29] or temporal modes [30, 31] (see Section VI of the Supplement). The GHZ-state version is achievable now with achieved squeezing levels (5 dB) in current technology [31]. Proof-of-principle experiments with a surface-code state are possible with ~ 10 dB of squeezing, which is state of the art but achievable [31–33]. Higher squeezing would enable practical large-scale anonymous broadcasting.

Resource states could also be prepared in circuit-QED setups, either dynamically or by engineering a quadratic Hamiltonian between microwave cavities [34] that has the CV cluster state as the gapped ground state and then performing quadrature measurements to map it to a CV surface code [12]. Single-mode [35, 36] and two-mode [37–40] squeezing has already been demonstrated in these systems, and the SQUID-based controlling technology allows for very strong nonlinearities [41–43], enabling high squeezing (~ 13 dB) [44–47].

Conclusion.—We propose using large-scale continuous-variable topological quantum codes for the important practical task of anonymously broadcasting classical information, and we quantify the channel capacity and anonymity of the protocol in terms of its physical parameters. Large squeezing enables high-capacity broadcasting with strong anonymity, but there is a trade-off between the two for any fixed level of squeezing. Our protocol outperforms other anonymous broadcasting protocols in two crucial ways: (1) Because a topological quantum code serves as the resource, the scheme is robust to errors. (2) Because that code is a continuous-variable code, the technology required for large-scale resource generation is already available. A notable feature of our protocol using continuous variables (instead of qubits) is that with large enough squeezing, anonymity is maintained even with channel capacity $C > 1$ bit. This would enable other, more complex tasks such as anonymous yes/no voting [6] within a group of size $\leq C$.

Acknowledgments.—G.K.B. thanks James Wootton for discussions on the discrete variable protocol and thanks J. Dowling for comments. T.F.D. thanks Joseph Fitzsimons for useful suggestions about past work on anonymous communication. T.F.D. is supported by the Singapore National Research Foundation under NRF Award NRF-NRFF2013-01. N.C.M. is supported by the Australian Research Council under grant No. DE120102204.

Supplemental Information

I. INITIALIZATION OF THE ENCODED MODE

Given the exact nullifiers for the finitely squeezed CV cluster state on a square lattice [48],

$$\hat{\eta}_j = \frac{1}{\sqrt{2}} \left[s^{-1} \hat{q}_j + i s \left(\hat{p}_j - \sum_{k \in \mathcal{N}(j)} \hat{q}_k \right) \right], \quad (6)$$

the measured modes lie on the vertices and the face centers of the CV surface-code graph, while the unmeasured nullifiers lie on the edges [see Fig. 1(b) in the main text and Fig. 3 in this Supplement]. Consider an alternating sum of cluster-state nullifiers $\hat{\eta}_j$ centered on the nodes of a loop \mathcal{P}_j [e.g., every other node left to right through the middle of Fig. 3(a): ..., 72, 98, ...]. This sum is, of course, also a nullifier of the original CV cluster state. The overlapping \hat{q} terms have canceled, and the sum can be written (up to normalization)

$$-\frac{i}{\sqrt{|\mathcal{P}_j|}} \sum_{e_k \in \mathcal{P}_j} (-1)^k \hat{\eta}_k = \hat{f}_j - \frac{s}{\sqrt{2|\mathcal{P}_j|}} \sum_{e_k \in \mathcal{P}_j} (\hat{q}_{v_k^L} + \hat{q}_{v_k^R}), \quad (7)$$

where $\hat{q}_{v_k^{L(R)}}$ are the position operators for the modes to the left (right) of the edge e_k , and they are located at the faces of the CV toric code (e.g., nodes 71, 73, 97, 99). Since these modes are measured in the \hat{q} basis we have a record of their values $\{q_{v_k^L}, q_{v_k^R}\}$. Call the accumulated value

$$Q_j = \frac{s}{\sqrt{2|\mathcal{P}_j|}} \sum_{e_k \in \mathcal{P}_j} (q_{v_k^L} + q_{v_k^R}). \quad (8)$$

Then, the prepared ground state is a displaced ground state of the string modes:

$$(\hat{f}_1 - Q_1)|\text{GS}\rangle = (\hat{f}_2 - Q_2)|\text{GS}\rangle = 0. \quad (9)$$

Henceforth, we will assume $Q_1 = Q_2 = 0$ because the displacement can be accounted for in the protocol by subtracting the value Q_2 when inferring the broadcast message.

If another method is used to prepare the CV toric code state—i.e., not beginning with the CV cluster state—then one would need to initialize the string modes in the ground state by other means. Call the CV toric-code state $\hat{\rho}$, where the string modes could be in any mixed state. Then, a possible method of cooling is to subject the system to decay governed by the following Liouvillian:

$$\hat{\mathcal{L}}_{\text{prep}}[\hat{\rho}] = \frac{\partial \hat{\rho}}{\partial t} = - \sum_{j=1}^2 (\hat{f}_j^\dagger \hat{f}_j \hat{\rho} + \hat{\rho} \hat{f}_j^\dagger \hat{f}_j). \quad (10)$$

The engineering of such dissipative maps on lattices of bosons was considered in Ref. [49]. The fixed point of this map is the CV toric code with the unconstrained modes in the ground state.

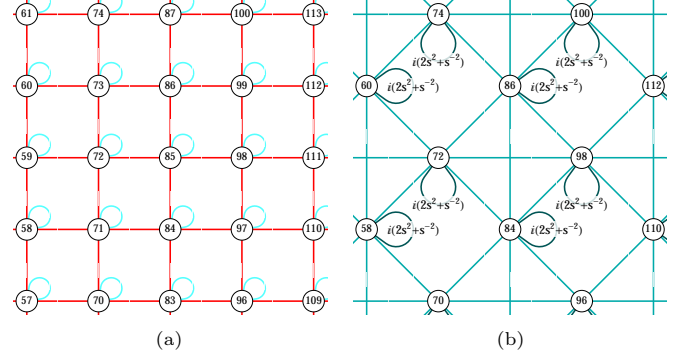


FIG. 3: Toroidal CV cluster state and toroidal CV surface-code state [12]. (a) Portion of a CV cluster state with toroidal boundary conditions. Red edges have weight 1, and cyan self-loops have weight $i s^{-2}$ [48]. (b) Portion of a CV surface-code state with toroidal boundary conditions (CV toric-code state). Unlabeled edges all have weight $i s^2$. This state is generated by measuring \hat{p} and \hat{q} on the odd nodes of (a) in a diagonally alternating pattern. The \hat{p} measurements delete the node and produce a criss-cross pattern in (b) where the node used to be. The \hat{q} measurements just delete the node. (In this case, \hat{q} was measured on nodes 71, 73, 97, 99; \hat{p} was measured on the other visible odd-numbered nodes; and so on.)

II. MEASUREMENT COVARIANCE MATRIX

In order to calculate the broadcast channel capacity (Section III) and the sender anonymity (Section IV), we need the covariance matrix of the players' messages. In this section we calculate this quantity *before* any broadcast is sent.

A. General formulation

We prepare a CV toric-code state via measurements on a canonical CV cluster state, as described in Ref. [12]. In this case, the vertex nullifiers deviate slightly from those discussed in the main text:

$$\hat{a}_v = \frac{1}{\sqrt{8}} \left(\sum_{+} (\tilde{s} \hat{q}_e + i \tilde{s}^{-1} \hat{p}_e) + s^2 \tilde{s}^{-1} \sum_{\diamond} \hat{q}_e \right). \quad (11)$$

(with some simple modifications if on a surface with boundary), where $\tilde{s} = \sqrt{5s^2 + s^{-2}}$, and \diamond means the diamond shaped loop of next nearest neighbours to the vertex v . However, everything in the protocol works the same as with the symmetric form \hat{a}_v . In particular $[\hat{a}_v, \hat{b}_f] = [\hat{a}_v, \hat{b}_f^\dagger] = 0$, and the string symmetries of the ground state subspace are the same (see [12]).

Figure 6 of Ref. [12] shows the Gaussian graph [48] for the CV surface code created from a canonical CV cluster state, which is also reproduced here in Figure 3(b). Since its graph $\mathbf{Z} = i\mathbf{U}$ is purely imaginary, it directly encodes the \hat{p} - \hat{p} correlations [48]: $\langle \hat{\mathbf{p}} \hat{\mathbf{p}}^T \rangle = \frac{1}{2} \mathbf{U}$.

When using this state for anonymous broadcasting,

\mathcal{P}_2 is left to right along one of these horizontal lines—e.g., ..., 72, 98, ... in Figure 3(b). We can write each player's measurement operator \hat{M}_j along a portion $\mathcal{P}_2(j)$ of this path as the inner product between the vector of momentum operators $\hat{\mathbf{p}}$ and a normalized indicator vector $\ell_j = |\mathcal{P}_2(j)|^{-1/2} \lambda_j$, where all entries of λ_j are ± 1 or 0. Assuming the width of each wedge is w , then

$$\hat{M}_j = \ell_j^T \hat{\mathbf{p}} = \frac{1}{\sqrt{w}} \lambda_j^T \hat{\mathbf{p}}. \quad (12)$$

Therefore, with respect to the original resource state (i.e., before any displacements intended to broadcast a message),

$$\begin{aligned} \langle \hat{M}_j \hat{M}_k \rangle &= \ell_j^T \langle \hat{\mathbf{p}} \hat{\mathbf{p}}^T \rangle \ell_k \\ &= \frac{1}{w} \lambda_j^T \left(\frac{1}{2} \mathbf{U} \right) \lambda_k \\ &= \frac{1}{2w} \text{tr}(\mathbf{U} \lambda_k \lambda_j^T). \end{aligned} \quad (13)$$

We can also consider the total measurement $\hat{M} = \ell^T \hat{\mathbf{p}} = |\mathcal{P}_2|^{-1/2} \lambda^T \hat{\mathbf{p}}$. Assuming n players and a width- w wedge given to each player,

$$(\Delta M)^2 := \langle \hat{M}^2 \rangle = \frac{1}{2nw} \text{tr}(\mathbf{U} \lambda \lambda^T). \quad (14)$$

To illustrate the use of these formulas, it will be helpful to analyze a simpler case first.

B. Simple case: 4-mode CV GHZ state

Consider the linear CV cluster state in Figure 4(a). By measuring \hat{p} on all even nodes, this state becomes the CV GHZ state whose Gaussian graph \mathbf{Z} [48] is shown in Figure 4(b). Forming its adjacency matrix—also called \mathbf{Z} without ambiguity by taking the nodes in numerical order—we get $\mathbf{Z} = i\mathbf{U}$ with

$$\mathbf{U} = \begin{pmatrix} s^2 + s^{-2} & s^2 & 0 & 0 \\ s^2 & 2s^2 + s^{-2} & s^2 & 0 \\ 0 & s^2 & 2s^2 + s^{-2} & s^2 \\ 0 & 0 & s^2 & s^2 + s^{-2} \end{pmatrix}. \quad (15)$$

We postulate two players using this state for broadcasting:

$$\hat{M}_1 := \frac{1}{\sqrt{2}}(\hat{p}_1 - \hat{p}_3), \quad (16)$$

$$\hat{M}_2 := \frac{1}{\sqrt{2}}(\hat{p}_5 - \hat{p}_7). \quad (17)$$

Therefore,

$$\lambda_1 = \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}, \quad \lambda_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix}. \quad (18)$$

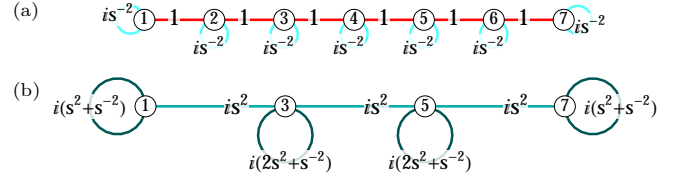


FIG. 4: (a) Linear CV cluster state and (b) CV GHZ state, with all edge weights labeled explicitly. Measuring \hat{p} on the even nodes in (a) produces (b). Notice that the self-loops at the ends of the GHZ state have a different weight from the ones in the middle.

The trace in the final form of Eq. (13) is just the Hilbert-Schmidt inner product (entry-wise inner product) between \mathbf{U} and $\lambda_j \lambda_k^T$. The relevant matrices are

$$\lambda_1 \lambda_1^T = \begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad (19)$$

$$\lambda_1 \lambda_1^T = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix}, \quad (20)$$

$$\lambda_1 \lambda_2^T = \begin{pmatrix} 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \quad (21)$$

Taking entry-wise inner products of these with \mathbf{U} , we can see that

$$\begin{aligned} \langle \hat{M}_1^2 \rangle &= \langle \hat{M}_2^2 \rangle = \frac{1}{4} [(s^2 + s^{-2}) + (2s^2 + s^{-2}) - 2s^2] \\ &= \frac{s^2}{4} + \frac{1}{2s^2}, \end{aligned} \quad (22)$$

and

$$\langle \hat{M}_1 \hat{M}_2 \rangle = \langle \hat{M}_2 \hat{M}_1 \rangle = \frac{-s^2}{4}. \quad (23)$$

The total measurement \hat{M} has $\lambda = \lambda_1 + \lambda_2$. Therefore,

$$\lambda \lambda^T = \begin{pmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{pmatrix}, \quad (24)$$

and the resultant entry-wise inner product with \mathbf{U} is the sum of the diagonal of \mathbf{U} minus all entries on the sub- and superdiagonals:

$$\begin{aligned} (\Delta M)^2 &= \langle \hat{M}^2 \rangle = \frac{1}{8} [2(s^2 + s^{-2}) + 2(2s^2 + s^{-2}) - 6s^2] \\ &= \frac{1}{2s^2}. \end{aligned} \quad (25)$$

Notice that all of the large-variance terms ($\sim s^2$) cancel in this sum. (The fact that the self-loops at the ends are different from those in the center of the chain is required for this cancelation to happen.) Therefore, the total measurement has a small variance even though individual players' measurements have a large variance—this is the essence of the anonymous broadcasting protocol.

C. CV toric-code state

We now return to the case of the toric-code state shown in Figure 3(b). We assume a general scenario of n players, each of whom possesses a slice of the torus of width w . Because of the toroidal boundary conditions, nw must be even, and we assume it is not trivially small (i.e., $nw \geq 4$).

For illustration, we start with the concrete example of $w = 4$. Then,

$$\lambda_j = (0 \cdots 0 \ 1 \ -1 \ 1 \ -1 \ 0 \cdots 0)^T, \quad (26)$$

where the nodes with nonzero entries are numbered along \mathcal{P}_2 . Since any node not along \mathcal{P}_2 corresponds to a 0 in all of the λ_j , we can consider just the induced subgraph of \mathbf{U} restricted to \mathcal{P}_2 —in other words, the submatrix of \mathbf{U} restricted to the nodes along \mathcal{P}_2 .

Inspection reveals that along \mathcal{P}_2 , \mathbf{U} for the toric code [Figure 3(b)] is exactly like that of the GHZ state [Figure 4(b)] except at the ends, where there is an extra edge connecting the two endpoints and self-loops of weight $2s^2 + s^{-2}$ instead of $s^2 + s^{-2}$. Continuing with the example above (and omitting zeros),

$$\lambda_j \lambda_k^T = \begin{pmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{pmatrix}, \quad (27)$$

with the size of the padding on each side (representing zeros) left unspecified but determined by j and k .

The relevant part of \mathbf{U} is *circulant* tridiagonal (nodes numbered according to \mathcal{P}_2) with all diagonal entries $2s^2 + s^{-2}$ (no difference at the ends because of periodicity) and all sub- and superdiagonal entries (continued in a circulant fashion) equal to s^2 :

$$\mathbf{U} \mapsto \begin{pmatrix} a & s^2 & & s^2 \\ s^2 & a & s^2 & \\ & \ddots & \ddots & \ddots \\ & & s^2 & a & s^2 \\ s^2 & & & s^2 & a \end{pmatrix}, \quad (28)$$

where $a = 2s^2 + s^{-2}$, nodes are again ordered according to their appearance along \mathcal{P}_2 , and \mapsto indicates that only the relevant part of the full \mathbf{U} is shown [cf. Eq. (15)].

When $j = k$, the 4×4 block of ± 1 in Eq. (27) is on the diagonal, and thus only the three innermost diagonals of that block matter when taking the entry-wise inner product with \mathbf{U} . Therefore, for $w = 4$, $\langle \hat{M}_j^2 \rangle = \frac{1}{8}[4(2s^2 + s^{-2}) - 6s^2]$. When $j - k = \pm 1 \pmod{n}$, then the only entry that matters is the -1 in the upper right or bottom left of the block, and thus $\langle \hat{M}_j \hat{M}_{j\pm 1} \rangle = \frac{1}{8}(-s^2)$. Analogous results hold for other even values of w , but we will postpone the general formula until we consider the odd case.

When w is odd, the form of the number block in Eq. (27) differs depending on whether $j - k$ is even or odd. This is because adjacent measurement operators have opposite sign configurations when adding up the individual \hat{p} operators. Using $w = 3$ as an example,

$$\lambda_j \lambda_{j+\text{even}}^T = \begin{pmatrix} 1 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}, \quad (29)$$

$$\lambda_j \lambda_{j+\text{odd}}^T = \begin{pmatrix} -1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & -1 \end{pmatrix}. \quad (30)$$

Notice that, once again, for the same reasons as for even w , only the cases where $j = k$ or $j - k = \pm 1 \pmod{n}$ matter, and now the pattern for both even and odd w is clear (and the same in both cases):

$$\begin{aligned} \langle \hat{M}_j^2 \rangle &= \frac{1}{2w} [w(2s^2 + s^{-2}) - 2(w-1)s^2] \\ &= \frac{1}{2s^2} + \frac{s^2}{w}, \end{aligned} \quad (31)$$

$$\langle \hat{M}_j \hat{M}_{j\pm 1} \rangle = \frac{-s^2}{2w}, \quad (32)$$

where the ± 1 is mod n . These are the pre-broadcast covariances of the players' measurement operators using a toric-code state. They also hold for the GHZ state with periodic boundary conditions, which is a special case of the torus.

The total measurement \hat{M} has a matrix $\lambda \lambda^T$ whose nonzero block is $nw \times nw$ and of the same form as Eq. (24). Notice that in order to get the periodicity to match up, nw must be even. Examining the form of \mathbf{U} in Eq. (28), we see that we must add the diagonal of \mathbf{U} and subtract its sub- and superdiagonals, including their circulant extensions (the entries in the corners). Therefore, we have the general result

$$\begin{aligned} (\Delta M)^2 = \langle \hat{M}^2 \rangle &= \frac{1}{2nw} [nw(2s^2 + s^{-2}) - 2nw(s^2)] \\ &= \frac{1}{2s^2}, \end{aligned} \quad (33)$$

which holds for all n and w (with $nw \geq 4$ and even).

D. CV surface-code state with open boundaries

The calculations of broadcast channel capacity (Section III) and sender anonymity (Section IV) assume a toric-code state, whose results were presented above. The optical implementation (Section VI), however, proposes implementing the protocol using surface-code states with open boundaries instead. Here we show that this sort of resource also works.

The open-boundary surface-code state is shown in Figure 5(b), where the top and bottom are ‘smooth’ boundaries, and the left and right are ‘rough’ boundaries, chosen by convention because of their visual representation in the graph. We can choose \mathcal{P}_2 to be any of the three horizontal lines of nodes in that graph that stretch all the way from the left boundary (rough) to the right boundary (also rough)—e.g., 3, 13, 23, 33. Alice will apply her displacements along $\tilde{\mathcal{P}}_2$, which could be, for instance, 11, 13, 15, or any of the vertical lines parallel to that one and that stretch all the way from the bottom boundary (smooth) to the top boundary (also smooth).

Notice that the self-loops at the rough boundaries [Figure 5(b)] are like the endpoints of the CV GHZ state [Figure 4(b)]. In fact, by the same logic as in the toric-code case above, the only part of \mathbf{U} that will matter is the submatrix of the full \mathbf{U} limited to the nodes along \mathcal{P}_2 . This now has the exact same form as the \mathbf{U} for the GHZ state, which is given in Eq. (15). For arbitrary n and w (with $nw \geq 4$ and even), this becomes

$$\mathbf{U} \mapsto \begin{pmatrix} b & s^2 & & & \\ s^2 & a & s^2 & & \\ & \ddots & \ddots & \ddots & \\ & & s^2 & a & s^2 \\ & & & s^2 & b \end{pmatrix}, \quad (34)$$

where $a = 2s^2 + s^{-2}$ and $b = s^2 + s^{-2}$, and \mapsto again indicates that only the relevant part of \mathbf{U} is displayed. Notice the two differences between this and Eq. (28): In Eq. (34), the first and last diagonal entries are different from the rest, and the isolated corner entries are missing.

Using the same arguments as above, we have the following nonzero covariance terms:

$$\begin{aligned} \langle \hat{M}_1^2 \rangle &= \langle \hat{M}_n^2 \rangle = \frac{1}{2w} [(w-1)(2s^2 + s^{-2}) \\ &\quad + (s^2 + s^{-2}) - 2(w-1)s^2] \\ &= \frac{1}{2s^2} + \frac{s^2}{2w}, \end{aligned} \quad (35)$$

$$\begin{aligned} \langle \hat{M}_j^2 \rangle &= \frac{1}{2w} [w(2s^2 + s^{-2}) - 2(w-1)s^2] \\ &= \frac{1}{2s^2} + \frac{s^2}{w}, \end{aligned} \quad (36)$$

$$\langle \hat{M}_j \hat{M}_{j\pm 1} \rangle = \frac{-s^2}{2w}, \quad (37)$$

where $2 \leq j \leq n-1$. Notice that the ± 1 is no longer

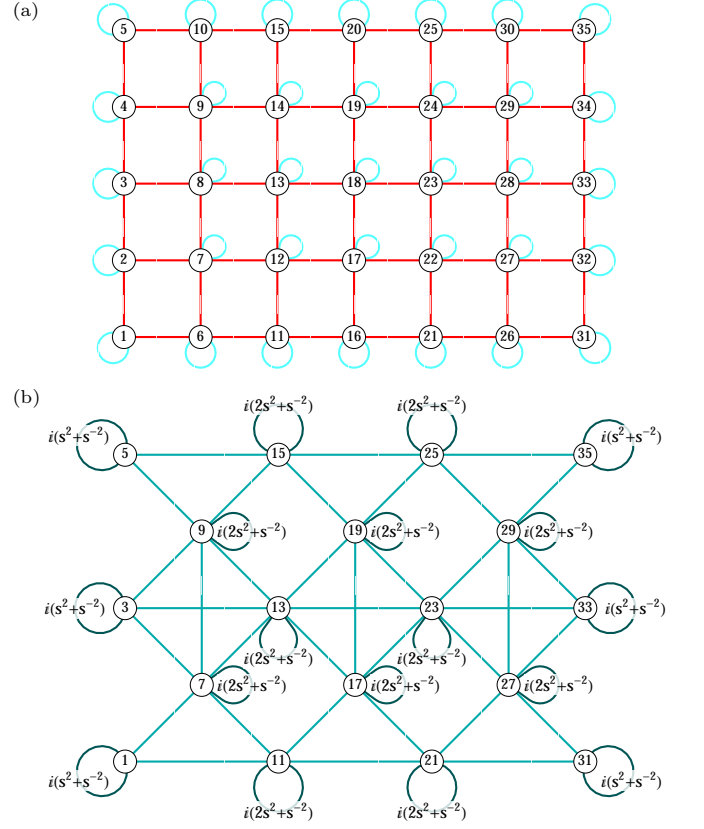


FIG. 5: Open-boundary CV cluster state and CV surface-code state. (a) CV cluster state with open boundaries. Red edges have weight 1, and cyan self-loops have weight is^{-2} [48]. (b) CV surface-code state with smooth boundaries on the top and bottom and with rough boundaries on the left and right. Unlabeled edges all have weight is^2 . Starting from (a), the smooth boundaries are generated by measuring \hat{p} on nodes 6, 16, 26, 10, 20, 30. The rough boundaries are generated by measuring \hat{q} on nodes 2, 4, 32, 34. An alternating pattern of \hat{p} and \hat{q} measurements on all remaining even nodes completes the transition to the surface-code state. (The terms ‘smooth’ and ‘rough’ are chosen by convention to visually match the boundaries of the resulting graph.) Also notice that the three horizontal lines extending the full width of (b) have the same weights as the CV GHZ state from Figure 4(b).

mod n . Also,

$$\begin{aligned} (\Delta M)^2 &= \langle \hat{M}^2 \rangle = \frac{1}{2nw} [(nw-2)(2s^2 + s^{-2}) \\ &\quad + 2(s^2 + s^{-2}) - 2(nw-1)s^2] \\ &= \frac{1}{2s^2}. \end{aligned} \quad (38)$$

In this case, the noise of the broadcast message is the same, $(\Delta M)^2 = \frac{1}{2s^2}$, which means the channel capacity is the same (Section III). But now players 1 and n are more at risk of being discovered if one of them is the broadcaster. This is because the local noise in their measurement outcomes is less than that of the other players,

and it is this local noise that hides the fact that any individual player has broadcast a message (Section IV).

One might be tempted to think that making the end wedges (1 and n) narrower, with a width of $\frac{w}{2}$ instead of w , could make the local noise the same for all players. This is true—but misleading. The reason for this is that if player 1 or n wanted to broadcast a message R , her measurement outcome would be displaced further than would players $2, \dots, n-1$ if one of them instead had broadcast the same message—in fact, further by a factor of $\sqrt{2}$ [see Eq. (45)]. This means that the variance of that displacement is twice what it would be had she used a full w -width wedge. This effectively nullifies the advantage of increased local noise in the narrower wedge. Either way, the local signal-to-noise ratio (which governs the risk of broadcaster discovery; see Section IV) is approximately twice what it would be for any of the other players wishing to broadcast the same message. Thus, there is no advantage to using narrower wedges at the ends.

III. BROADCAST CHANNEL CAPACITY

In this section, we calculate the channel capacity for the broadcast channel. We do not consider the anonymity of the broadcast (discussed in Section IV) but only how much information can be broadcast in one iteration of the protocol. Since the message space is unbounded, the capacity is technically infinite. Therefore, in order to get a finite quantity, we will actually calculate the channel capacity conditioned on a fixed variance τ^2 of the message to be broadcast. (This does not specify the shape of the broadcast message distribution, of course, since two possibilities would be a Gaussian with variance τ^2 and a binary distribution with δ -function support only at $\pm\tau$.)

For an input message $R \in \mathbb{R}$ and some output reconstructed message $M \in \mathbb{R}$, the variance-restricted channel capacity is $C = \max_{p_R(r)} I(R; M)$, where the maximum is over all input probability distributions $p_R(r)$ with variance τ^2 , and $I(R; M) = H(M) - H(M|R)$ is the mutual information between R and M [50]. The conditional probability $p_{M|R}(m|r) = N_{m,(\Delta M)^2}(r)$ is a normal distribution in output m with mean r and variance $(\Delta M)^2$ from Eq. (33).

For an arbitrarily distributed R with mean μ and variance τ^2 , the cumulant vector [51] for R is $\mathbf{c}_R = (\mu, \tau^2, c_3, c_4, \dots)$, and that for M is called \mathbf{c}_M . Using the law of total probability,

$$\begin{aligned} p_M(m) &= \int dr p_{M|R}(m|r) p_R(r) \\ &= (N_{0,(\Delta M)^2} * p_R)(m), \end{aligned} \quad (39)$$

where $*$ indicates convolution. Cumulants add under

convolution [51]. Therefore,

$$\begin{aligned} \mathbf{c}_M &= \mathbf{c}_R + (0, (\Delta M)^2, 0, \dots) \\ &= (\mu, \tau^2 + (\Delta M)^2, c_3, c_4, \dots). \end{aligned} \quad (40)$$

Note that $H(M|R)$ is fixed by the channel since $p_{M|R}(m|r)$ is a function only of $(m-r)$, and thus averaging over R does not change the entropy. Therefore, the only difference that p_R makes to $I(R; M)$ is through $H(M)$. We can maximize $I(R; M)$ by maximizing $H(M)$ (subject to the τ^2 constraint), which means requiring that p_M be Gaussian (see Section VII) with variance $\tau^2 + (\Delta M)^2$ and arbitrary mean. This can be achieved by requiring all cumulants beyond the second of \mathbf{c}_M to be zero—i.e., $\mathbf{c}_M = (\mu, \tau^2 + (\Delta M)^2, 0, 0, \dots)$. Therefore, $\mathbf{c}_R = (\mu, \tau^2, 0, 0, \dots)$, which means that the maximizing p_R is also Gaussian. For a given variance τ^2 of the message, this choice maximizes the mutual information and thus defines the (variance-restricted) channel capacity (see Section VII):

$$\begin{aligned} C &= \frac{1}{2} \log[2\pi e(\tau^2 + (\Delta M)^2)] - \frac{1}{2} \log[2\pi e(\Delta M)^2] \\ &= \frac{1}{2} \log(1 + \alpha), \end{aligned} \quad (41)$$

where $\alpha = \frac{\tau^2}{(\Delta M)^2}$ is the signal-to-noise ratio (SNR) of the broadcast.

IV. SENDER ANONYMITY

In this section we quantify the anonymity of the broadcast channel in terms of how much information about the identity of the sender leaks out into the classical measurement record. We assume a surface-code state with toroidal boundary conditions, as presented in the main text and discussed in Section II C, in order to simplify the calculation by putting all players on the same footing. A similar calculation is possible using other boundary conditions and more general assumptions, but our purpose is simply to quantify the amount of anonymity in a basic instance of the protocol.

A. Players' measurements covariance matrix after broadcast

In Section II C, we calculated the covariance matrix of the players' individual measurement outcomes before any broadcast is made (which we now call \bar{M}_j):

$$\langle \bar{M}_j^2 \rangle = \frac{1}{2s^2} + \frac{s^2}{w}, \quad (42)$$

$$\langle \bar{M}_j \bar{M}_{j\pm 1} \rangle = \frac{-s^2}{2w}, \quad (43)$$

and all other covariances are 0. As such, the full covariance matrix for the random measurement-results vector $\bar{\mathbf{M}}$ can be written using the definition for the circulant matrix in Section VII, Eq. (87):

$$\bar{\Sigma} := \langle \bar{\mathbf{M}}\bar{\mathbf{M}}^T \rangle = \frac{-s^2}{2w} \mathbf{C}_n \left(-\frac{w}{s^4} - 2 \right). \quad (44)$$

Let the identity of Alice (the broadcaster) be associated with a random variable $A \in \{1, \dots, n\}$. (It is random because other people wishing to discover her identity do not know who she is.) We assume that she wishes to broadcast a real number $r \in \mathbb{R}$, which we shall treat as an instantiation of a Gaussian-distributed random variable $R \sim N_{0,\tau^2}(r)$, as is prescribed to be optimal in Section III. Conditioned on Alice actually being player a , applying the string-operator shift along $\tilde{\mathcal{P}}_2$ to implement the broadcast, the actual random measurement outcome for each player can be written

$$M_{j|a} := \bar{M}_j + \sqrt{n}R\delta_{ja}, \quad (45)$$

since $n = |\mathcal{P}_2|/|\mathcal{P}_2(j)|$. Then, the variance and covariance of the actual measurement outcomes *when averaged over the actual message sent* are, respectively,

$$\langle M_{j|a}^2 \rangle = \frac{1}{2s^2} + \frac{s^2}{w} + n\tau^2\delta_{ja}, \quad (46)$$

$$\langle M_{j|a}M_{j\pm 1|a} \rangle = \frac{-s^2}{2w}. \quad (47)$$

This gives the following covariance matrix of the actual random vector of outcomes, conditioned on the broadcaster being player a :

$$\Sigma_{|a} := \langle \mathbf{M}_{|a}\mathbf{M}_{|a}^T \rangle = \bar{\Sigma} + n\tau^2\mathbf{e}_{aa}, \quad (48)$$

where \mathbf{e}_{aa} is a matrix with a 1 in the (a, a) entry and zeros everywhere else.

B. Leakage of information about broadcaster's identity

We model the leakage of information about the broadcaster's identity in terms of the mutual information $I(\mathbf{M}; A)$ between the random vector of measurement outcomes \mathbf{M} (averaged over the broadcaster A and the message R) and the random variable A identifying the broadcaster [50]. In other words, how much information about A can be extracted from \mathbf{M} ? More specifically, this measures how much the entropy of A is reduced (on average) if one has access to the measurement record \mathbf{M} :

$$I(\mathbf{M}; A) = H(A) - H(A|\mathbf{M}). \quad (49)$$

Symmetry of the mutual information means that we can also write it as

$$I(\mathbf{M}; A) = H(\mathbf{M}) - H(\mathbf{M}|A), \quad (50)$$

which will be more straightforward to calculate.

The conditional entropy is the entropy of \mathbf{M} if one knows who the broadcaster is, averaged over both the message and the broadcaster's identity:

$$H(\mathbf{M}|A) = \langle -\log p_{\mathbf{M}|A}(\mathbf{M}|A) \rangle_{\mathbf{M},A}. \quad (51)$$

We assume, for simplicity, that we have no initial information about the broadcaster's identity—a flat prior over all possible broadcasters:

$$A \sim p_A(a) = \frac{1}{n}. \quad (52)$$

From the subsection above, we know the distribution of the message $\mathbf{M}_{|a}$ conditioned on knowing who the broadcaster is:

$$\mathbf{M}_{|a} \sim p_{\mathbf{M}|A}(\mathbf{m}|a) = N_{\mathbf{0},\Sigma_{|a}}(\mathbf{m}). \quad (53)$$

Therefore (see Section VII),

$$\begin{aligned} H(\mathbf{M}|A) &= \left\langle \frac{1}{2} \log \det (2\pi e \Sigma_{|A}) \right\rangle_A \\ &= \frac{1}{2} \log \det [2\pi e (\bar{\Sigma} + n\tau^2\mathbf{e}_{1,1})]. \end{aligned} \quad (54)$$

Note that $n\tau^2$ could have just as well been added to any other location on the diagonal; the $(1,1)$ entry was chosen by fiat.

Using the law of total probability, we can calculate

$$\begin{aligned} \mathbf{M} \sim p_{\mathbf{M}}(\mathbf{m}) &= \sum_{a=1}^n p_{\mathbf{M}|A}(\mathbf{m}|a)p_A(a) \\ &= \frac{1}{n} \sum_{a=1}^n N_{\mathbf{0},\Sigma_{|a}}(\mathbf{m}). \end{aligned} \quad (55)$$

This is not a Gaussian; rather, it is a mixture of Gaussians with different covariance matrices. Nevertheless, we can use the law of total expectation to calculate

$$\begin{aligned} \Sigma &:= \langle \mathbf{M}\mathbf{M}^T \rangle_{\mathbf{M}} \\ &= \frac{1}{n} \sum_{a=1}^n \langle \mathbf{M}_{|a}\mathbf{M}_{|a}^T \rangle_{\mathbf{M}|a} \\ &= \frac{1}{n} \sum_{a=1}^n \Sigma_{|a} \\ &= \bar{\Sigma} + \tau^2\mathbf{I} \end{aligned} \quad (56)$$

By Eq. (85) in Section VII, we can use this to place an upper bound on $H(\mathbf{M})$:

$$H(\mathbf{M}) \leq \frac{1}{2} \log \det [2\pi e (\bar{\Sigma} + \tau^2\mathbf{I})]. \quad (57)$$

And hence, combining Eqs. (54) and (57), we have

$$I(\mathbf{M}; A) \leq \frac{1}{2} \log \left[\frac{\det(\bar{\Sigma} + \tau^2\mathbf{I})}{\det(\bar{\Sigma} + n\tau^2\mathbf{e}_{1,1})} \right]. \quad (58)$$

Using ϵ and α from Eq. (4) of the main text, repeated here for reference,

$$\epsilon = \frac{(\Delta M)^2}{(\Delta M_j)^2 - (\Delta M)^2}, \quad \alpha = \frac{\tau^2}{(\Delta M)^2}, \quad (59)$$

we can write

$$\bar{\Sigma} + \tau^2 \mathbf{I} = \frac{-s^2}{2w} \mathbf{C}_n [-2(1 + \epsilon + \epsilon\alpha)], \quad (60)$$

$$\bar{\Sigma} + n\tau^2 \mathbf{e}_{1,1} = \frac{-s^2}{2w} \mathbf{C}_n [-2(1 + \epsilon), -2n\epsilon\alpha]. \quad (61)$$

Using Eqs. (94), and (97) in Section VII, we obtain an explicit bound on the amount of information about the broadcaster's identity leaked within the measurement outcomes (assuming $n \geq 3$):

$$I(\mathbf{M}; A) \leq \frac{1}{2} \log \left\{ \frac{T_n(1 + \epsilon + \epsilon\alpha) - 1}{(1 + \epsilon\alpha \frac{\partial}{\partial \epsilon}) [T_n(1 + \epsilon) - 1]} \right\}. \quad (62)$$

The mathematical form of Eq. (62) can be interpreted as comparing a shift in a function [namely, $f(\epsilon) \mapsto f(\epsilon + \epsilon\alpha)$, where $f(\epsilon) = T_n(1 + \epsilon) - 1$] to its first-order Taylor-series approximation. When this is a good approximation, anonymity is high, and little identifying information leaks out.

The only reason Eq. (62) is not an equality is that we used the fact that the entropy of a mixture of Gaussians is upper bounded by the entropy of a Gaussian with the same covariance as that of the mixture. When this is a bad approximation, it is possible that the right-hand side of Eq. (62) could exceed $H(A) = \log n$, while the actual value of $I(\mathbf{M}; A)$ never will.

Also note that $I(\mathbf{M}; A)$ as calculated is not additive under multiple repetitions of the protocol because after each run, the prior $p_A(a)$ about the sender's identity will have changed based on the new information, requiring a new calculation. Nevertheless, for a single instance of the protocol, Eq. (62) quantifies the lack of anonymity of the broadcaster.

Anonymity is high whenever Alice's post-broadcast probability of discovery is very low:

$$1 \gg 2^{-H(A|\mathbf{M})} = \frac{2^{I(\mathbf{M}; A)}}{2^{H(A)}}, \quad (63)$$

using log base 2. Replacing $I(\mathbf{M}; A)$ in Eq. (63) with its upper bound from Eq. (62) and then squaring both sides only strengthens the condition, which lets us write the following in the limit of a good resource state ($\epsilon \ll 1$):

$$n^2 \gg 1 + \frac{(n^2 - 1)\alpha^2 \epsilon}{6(1 + \alpha)} + O(\epsilon^2). \quad (64)$$

Solving for α and dropping terms of $O(\epsilon^2)$ gives the bound reported in the main text:

$$\alpha \epsilon \ll 6. \quad (65)$$

Since $\alpha \epsilon$ is the SNR of the broadcast message to the excess noise in each of the local measurements, we can summarize this condition by saying that anonymity is high when the broadcast message is sufficiently obscured by the local measurement noise.

V. WEDGE WIDTH IN FIGURE 2

Figure 2 in the main text assumes that the players have received wedges of width $w = 6$. Here we justify this choice.

We assume the ancilla-based error suppression and detection scheme proposed in the main text. A detected ancillary photon decay event indicates an error in the code (a jump out of the code space) in the neighborhood of that vertex and face. We then logically tag that location as a part of the code to be avoided—effectively declaring that node lost completely. This is a conservative choice that allows us to steer clear of detected errors altogether.

For rates of lost (i.e., error-tagged) nodes below the toric-code error tolerance rate of 50% (error per mode $p_{\text{err}} = \frac{1}{2}$ per physical operation), as derived from the percolation threshold for a square lattice [52], paths can be found that connect the lattice along homologically non-trivial loops. Communication between parties restricts the allowable density of errors and defines a lower bound for the width of each wedge. For occupation probability p below the percolation threshold p_c , the probability that there is a cluster of radius r in the percolation model is given by $p_{\text{cluster}}(r) \approx e^{-r|p - p_c|^\nu}$ where ν is the critical exponent [53]. For bond percolation on a square lattice in two dimensions, $p_c = \frac{1}{2}$ and $\nu = \frac{4}{3}$, so the probability the protocol fails due to these errors is

$$p_{\text{fail}} \approx e^{-\frac{w}{2}|p_{\text{err}} - \frac{1}{2}|^{4/3}}. \quad (66)$$

Hence, for a target p_{fail} , we have

$$w \geq \frac{2 \log(p_{\text{fail}}^{-1})}{|p_{\text{err}} - \frac{1}{2}|^{4/3}}. \quad (67)$$

Assume errors can be monitored, for instance using the protocol described in the main text. Then, if one of the parties measures a percolated cluster of errors on her wedge, she can announce an abort warning to the others. The whole protocol can then be retried, and the probability of failure after k attempts is p_{fail}^k . Say we fix $p_{\text{fail}} = 1/e$, implying

$$w \geq \frac{2}{|p_{\text{err}} - \frac{1}{2}|^{4/3}}. \quad (68)$$

Then, assuming an error rate $p_{\text{err}} < 0.06$, a wedge width of $w = 6$ will suffice. This percolation argument also assumes a circumference of the wedge around the same size.

VI. OPTICAL IMPLEMENTATION

Here we detail the optical implementation mentioned in the main text.

A. Macrocode-based CV cluster states

Recent experimental results have shown that compact optical experimental setups can produce huge CV cluster states, including a 10,000-mode CV cluster state [31] with modes multiplexed in time (temporal modes) and a 60-mode CV cluster state [29] with modes multiplexed in frequency (frequency modes). These are cluster states with linear graphs, but the extension to a square lattice is straightforward and readily achievable with current technology [28, 48, 54].

These setups were already discussed in Ref. [12] as candidates for generating CV surface-code states like the ones necessary for this protocol. Here we review this construction and discuss its implementation for anonymous broadcasting.

The temporal-mode [30, 31] and frequency-mode [28, 29, 54, 55] construction methods generate a toroidal [54, 55] or cylindrical [28, 30] CV cluster state with a Gaussian graph [48] whose overall structure is that of a square lattice but is nevertheless not an ordinary lattice like in Fig. 3(a). Instead, it is a lattice based on 4-node groupings called *macronodes*, with a structure as shown in Fig. 6. The actual CV cluster state has the full graph [48]

$$\mathbf{Z} = i\delta\mathbf{I} + t\mathbf{G}, \quad (69)$$

where $\delta = \text{sech } 2r$, $t = \tanh 2r$, and \mathbf{G} is the graph shown in Fig. 6, with edge weights $\pm \frac{1}{4}$.

By measuring the top three modes of each macronode in \hat{q} , all but a single layer of the grid is deleted, leaving a uniformly-weighted, ordinary CV cluster state with graph [48]

$$\mathbf{Z}_{\text{CS}} = i\delta\mathbf{I} + g\mathbf{A}_{\text{grid}}, \quad (70)$$

where $\delta = \text{sech } 2r$, $g = \frac{1}{4}\tanh 2r$, $r > 0$ is an overall squeezing parameter, and \mathbf{A}_{grid} is a binary adjacency matrix for an ordinary square-lattice graph with boundary conditions (toroidal or cylindrical) inherited from its parent, Eq. (69). Note that the edge weights in \mathbf{Z}_{CS} are all $\frac{1}{4}\tanh 2r$, while in the canonical construction [shown in Fig. 3(a)] they should all be 1. Nevertheless, we can remodel the cluster state [12, 56] by redefining quadratures so that the edge weights are 1 but at a cost of multiplying the self-loop weights by g^{-1} . Since $\text{sech } 2r = \delta =: s_0^{-2}$, this means that the original value of s_0 (so labeled to differentiate it from the actual s used in the protocol) could be considered to be $s_0 = \sqrt{\cosh 2r}$, except for the non-unit g . The new effective value of s , which should be used in the calculations in the previous sections, is less

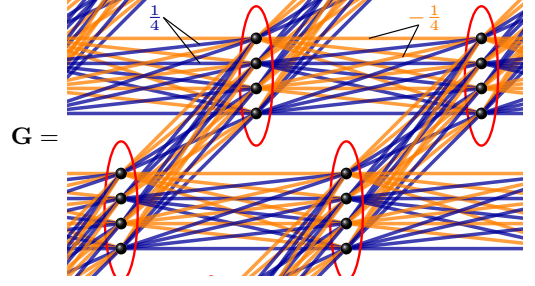


FIG. 6: Basic graph \mathbf{G} for temporal-mode CV cluster states [30]; the full graph [48] is given in Eq. (69). \mathbf{G} , as shown, also represents frequency-mode CV cluster states [28, 54, 55] up to trivial π phase shifts that merely flip the sign of some of the edges. Notice that \mathbf{G} has the overall structure of a square lattice [Fig. 3(a)], but the individual nodes of that lattice are now collections of 4 nodes called *macronodes*. Each macronode is identified by its surrounding red oval. In the temporal-mode case [30], each of the 4 nodes within a macronode is a synchronous temporal mode in four spatially separate laser beams. In the cylindrical frequency-mode case [28], each of the 4 nodes within a macronode share a common frequency but differ in spatial beam and polarization. The toroidal frequency-mode case [54, 55] is more complicated in structure and offers no advantages over the cylindrical one, so we do not consider it further.

than half this initial value [12, 56]:

$$s = \frac{s_0}{2} \sqrt{\tanh 2r} = \frac{1}{2} \sqrt{\sinh 2r}, \quad (71)$$

With a canonical CV cluster state obtained, which has uniform edge weight of 1, with s from Eq. (71), we can use local \hat{q} measurements to “cut and unroll” the cylinder or torus into a square lattice with the necessary smooth/rough boundary conditions as identified in Section IID. Further local \hat{q} and \hat{p} measurements are then used to convert this state to a CV surface code state [12] with two rough and two smooth edges as shown in Fig. 5(b), which is then distributed to the players. The broadcast protocol proceeds according to the modifications described in Section IID.

One might think we could take advantage of the cylindrical or toroidal structure of the original CV cluster states to produce a surface-code state with periodic boundaries. This fails, however, because the graphs of both states have a one-grid-unit twist along each compactified direction [28, 30, 55], which makes the checkerboard pattern of measurements needed to convert it into a cylindrical or toroidal surface code fail to line up properly. This is why we have to cut it into a surface code with open boundaries instead. If the twist were by an even number of grid units, other boundary conditions might be possible.

The temporal-mode scheme [30] claims an advantage over the cylindrical frequency-mode scheme [28] in terms of ease of distribution. This is because the temporal-

mode cylindrical lattice is built up like sequentially winding thread around a spool. This means that large chunks of the lattice are contiguous in time. Thus, one only needs a quickly adjustable mirror in order to distribute the pieces of the lattice to the players. Initially, the mirror is used to direct one of the four output beams to the first player. (The other three beams are immediately measured in \hat{q} to do the projection down to an ordinary lattice.) Once the player has received enough modes to form his/her sublattice, the mirror is switched so that the output beam is directed toward the second player, and so on. \hat{q} measurements at the start and end of this entire process are used to clean up the total lattice before the players themselves do the necessary additional \hat{q} and \hat{p} measurements to transform the state into a surface-code state. The “radius of the cylinder” in the temporal-mode case is limited by the coherence length L of the laser, but its width in the temporal direction—which is the direction used to measure the width w of each player’s wedge, for instance—is not so limited since far-separated modes do not need to directly interact. This means that the temporal-mode scheme is capable of involving a practically unlimited number of players.

The cylindrical frequency-mode scheme [28] has the same graph structure, but the frequencies of nearby modes are widely separated, so it is not as easy to split the lattice up into contiguous pieces for distribution. If this hurdle could be overcome, the frequency-mode scheme might claim an advantage because it is a continuous-wave scheme, meaning it might provide a means to transmit information continuously, rather than in bursts, as would be required by the temporal-mode scheme.

B. Squeezing levels for surface-code protocol

The rescaling of s shown in Eq. (71) means that this is likely not the most efficient way of generating a surface-code state, in terms of making good use of available squeezing resources [56]. Further theoretical work could lead to better procedures, but for now, we can look at the state of the art and what is achievable.

The largest squeezing achieved to date in these large-scale schemes is 5 dB in the temporal-mode experiment [31]. This corresponds to

$$r = \frac{\#dB}{20} \ln 10 \simeq 0.5756, \quad (72)$$

which means that the effective s for a protocol using this state is

$$s = \frac{1}{2} \sqrt{\sinh 2r} \simeq 0.5965, \quad (73)$$

which corresponds to an effective initial squeezing of

$$(\text{effective } \#dB) = 20 \log_{10} s \simeq -4.488 \text{ dB} \quad (74)$$

when doing the protocol. The negative sign means that this state is equivalent to a canonical CV cluster state [Fig. 3(a)] made with *anti-squeezed* vacuum modes (i.e., vacuum modes squeezed in the wrong direction) [48]. Note that this does not mean that we would be better off not doing any squeezing at all in the actual experiment. Instead, this is simply a side-effect of the straightforward, but squeezing-inefficient [12, 56], projection to an ordinary lattice from the macrocode-based lattice shown in Fig. 6. In this case, it produces a poor-quality state that is equivalent to one made with anti-squeezed input modes. Since we want $s^2 \gg 1$ for nontrivial channel capacity with high anonymity (Sections III and IV), either improved squeezing or further theoretical improvements in the protocol would be required to make practical use of these resources.

Single-mode squeezing as high as 12.7 dB has been achieved in optics experiments [32, 33], so it would be state of the art, but not unreasonable, to consider 10 dB achievable in temporal-mode [30, 31] or frequency-mode [28, 29] CV cluster states. Using Eqs. (72), (73), and (74), this corresponds to an effective squeezing of +0.925 dB, or an effective $s = 1.112$. This would still allow for semi-anonymous broadcasting—which we define as giving a probability $p < 2/n$ of the sender being correctly identified (less than twice the probability of random guessing). This would be possible when broadcasting 0.25 bits (corresponding to an SNR $\alpha = 0.414$) for $n \leq 11$ or broadcasting 0.5 bits ($\alpha = 1$) with $n \leq 5$. This would be enough for a proof-of-principle demonstration.

C. Squeezing levels for GHZ-state protocol

The calculations above assume that a full surface-code state is used as the resource. This has a macrocode-based graph with edge weights $\pm \frac{1}{4}$, as shown in Fig. 6, which reduces the effective squeezing dramatically when projected down to an ordinary lattice [56]. A surface code is necessary for error mitigation but not for basic demonstration of the protocol itself. For this, a simple GHZ state will suffice. As shown in Fig. 4, this can be made from a linear CV cluster state.

The basic graph \mathbf{G} for the actual state created in the temporal-mode experiment [31] is shown in Fig. 7, where the full graph \mathbf{Z} [48] is again obtained from \mathbf{G} through Eq. (69). This graph has 2-node macrocodes (instead of 4-node), and the edge weights are $\pm \frac{1}{2}$ (instead of $\pm \frac{1}{4}$), which means that with a base squeezing of 5 dB, the effective s for a protocol based on this linear resource [56] is larger than in the surface-code case [compare Eq. (73)]:

$$r \simeq 0.5756 \implies s = \frac{1}{\sqrt{2}} \sqrt{\sinh 2r} \simeq 1.006. \quad (75)$$

This corresponds to an effective initial squeezing of

$$(\text{effective } \#dB) = 20 \log_{10} s \simeq +0.05297 \text{ dB}, \quad (76)$$

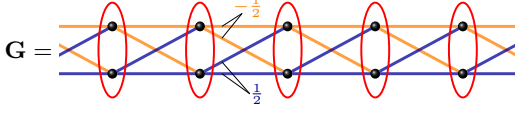


FIG. 7: Basic graph \mathbf{G} for the temporal-mode linear CV cluster state reported in [31]; the full graph \mathbf{Z} [48] is obtained from this through Eq. (69). \mathbf{G} , as shown, also represents frequency-mode CV cluster states reported in [29] up to trivial π phase shifts that merely flip the sign of some of the edges. Notice that \mathbf{G} has the overall structure of a line graph [Fig. 4(a)], but the individual nodes of that lattice are now collections of 2 nodes called *macronodes*. Each macronode is identified by its surrounding red oval. In the temporal-mode experiment [30, 31], each node within a macronode is a synchronous temporal mode in spatially separate laser beams. In the frequency-mode experiment [28, 29], each node is one of two polarizations with the same frequency.

which can be compared with Eq. (74).

With error correction not possible when using a GHZ state, we can reduce the wedge width w to its minimum value: $w = 1$. In this scenario, semi-anonymous broadcasting ($p < 2/n$; see subsection above) is possible for

$$C = 0.25 \text{ bits} \quad (\alpha = 0.414), \quad n \leq 17; \quad (77)$$

$$C = 0.5 \text{ bits} \quad (\alpha = 1), \quad n \leq 8; \quad (78)$$

$$C = 0.75 \text{ bits} \quad (\alpha = 1.828), \quad n \leq 5; \quad (79)$$

$$C = 1 \text{ bit} \quad (\alpha = 3), \quad n \leq 4. \quad (80)$$

Thus, optical technology available today [31] can be used to demonstrate a practical implementation of GHZ-state-based anonymous broadcasting using this protocol.

D. Scalability

The main advantage of these optical implementations remains in their immense scalability. CV GHZ states are already available today with current technology for anonymous broadcasting, and surface-code-based protocols are possible with state-of-the-art implementations. If the squeezing can be increased (or a more efficient conversion protocol devised), this technology holds great promise for large-scale anonymous broadcasting.

VII. MATHEMATICAL RESULTS

This section provides mathematical results that are used in Sections III and IV.

A. Gaussian distributions: notation and entropic properties

We adopt the following notation for a random variable X with instantiations $x \in \mathbb{R}$ distributed according to a Gaussian (normal) distribution with mean $\langle X \rangle = \mu$ and variance $\text{var}(X) = \langle (X - \mu)^2 \rangle = \sigma^2$:

$$X \sim N_{\mu, \sigma^2}(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp \left[-\frac{(x - \mu)^2}{2\sigma^2} \right]. \quad (81)$$

This can easily be extended to a random column vector \mathbf{X} with instantiations $\mathbf{x} \in \mathbb{R}^n$ distributed according to a multivariate Gaussian with mean $\langle \mathbf{X} \rangle = \boldsymbol{\mu}$ and covariance matrix $\text{cov}(\mathbf{X}) = \langle (\mathbf{X} - \boldsymbol{\mu})(\mathbf{X} - \boldsymbol{\mu})^T \rangle = \boldsymbol{\Sigma} > 0$:

$$\begin{aligned} \mathbf{X} &\sim N_{\boldsymbol{\mu}, \boldsymbol{\Sigma}}(\mathbf{x}) \\ &= \frac{1}{\sqrt{\det(2\pi\boldsymbol{\Sigma})}} \exp \left[-\frac{1}{2}(\mathbf{x} - \boldsymbol{\mu})^T \boldsymbol{\Sigma}^{-1}(\mathbf{x} - \boldsymbol{\mu}) \right]. \end{aligned} \quad (82)$$

The entropy of the univariate Gaussian is

$$H(X) = \langle -\log N_{\mu, \sigma^2}(X) \rangle = \frac{1}{2} \log(2\pi e \sigma^2). \quad (83)$$

Note that we leave the base unspecified. Therefore, all entropies in this document are expressed in bits if the log based is 2, in nats if the log base is e , etc. Its multivariate generalization is

$$H(\mathbf{X}) = \langle -\log N_{\boldsymbol{\mu}, \boldsymbol{\Sigma}}(\mathbf{X}) \rangle = \frac{1}{2} \log \det(2\pi e \boldsymbol{\Sigma}). \quad (84)$$

For any random vector \mathbf{Y} —not necessarily Gaussian—with mean $\boldsymbol{\mu}$ and covariance $\boldsymbol{\Sigma}$, its entropy is bounded from above by the entropy of a Gaussian-distributed random vector with the same covariance. In other words,

$$H(\mathbf{Y}) \leq \frac{1}{2} \log \det(2\pi e \boldsymbol{\Sigma}) = H(\mathbf{X}). \quad (85)$$

These formulas are used in Section III and Section IV.

B. Special cases of symmetric, tridiagonal, toeplitz/circulant matrices

Consider the two $n \times n$ matrices

$$\mathbf{T}_n(x) := \begin{pmatrix} x & 1 & & & \\ 1 & x & 1 & & \\ & 1 & x & 1 & \\ & & \ddots & \ddots & \ddots \\ & & & 1 & x & 1 \\ & & & & 1 & x & 1 \\ & & & & & 1 & x \end{pmatrix} \quad (86)$$

and

$$\mathbf{C}_n(x) := \begin{pmatrix} x & 1 & & & & & 1 \\ 1 & x & 1 & & & & \\ & 1 & x & 1 & & & \\ & & \ddots & \ddots & \ddots & & \\ & & & 1 & x & 1 & \\ & & & & 1 & x & 1 \\ 1 & & & & & 1 & x \end{pmatrix}, \quad (87)$$

with constant diagonal bands understood and missing entries taken to be 0. The notation is chosen because $\mathbf{T}_n(x)$ is a Toeplitz matrix and $\mathbf{C}_n(x)$ is its circulant counterpart. These matrices are uniquely defined for $n \geq 3$. We can complete the definition for all $n \in \mathbb{N}_+$ by also defining

$$\mathbf{T}_1(x) = \mathbf{C}_1(x) := (x), \quad (88)$$

$$\mathbf{T}_2(x) = \mathbf{C}_2(x) := \begin{pmatrix} x & 1 \\ 1 & x \end{pmatrix}. \quad (89)$$

Now let us consider their determinants.

Define $t_n(x) := \det \mathbf{T}_n(x)$. Using the cofactor expansion of the determinant, we see that the following recurrence relation holds for $n \geq 3$ [57, 58]:

$$t_n(x) = xt_{n-1}(x) - t_{n-2}(x). \quad (90)$$

Since $t_2(x) = x^2 - 1$ and $t_1(x) = x$ by direct calculation, we see that this recurrence relation also holds for $n = 2$ if we choose $t_0(x) := 1$. These are exactly the recurrence relation and initial conditions for the Chebyshev polynomials of the second kind $U_n(\frac{x}{2})$. Therefore,

$$\det \mathbf{T}_n(x) = t_n(x) = U_n\left(\frac{x}{2}\right). \quad (91)$$

This result also agrees with the literature [59–62] after applying properties of Chebyshev polynomials.

Define $c_n(x) := \det \mathbf{C}_n(x)$. A cofactor expansion for $n \geq 3$ relates this to the result for the Toeplitz case:

$$c_n(x) = xt_{n-1}(x) - 2[t_{n-2}(x) + (-1)^n]. \quad (92)$$

Plugging in Eq. (91) and using properties of Chebyshev polynomials gives

$$c_n(x) = 2(-1)^n \left[T_n\left(-\frac{x}{2}\right) - 1 \right], \quad (93)$$

where T_n is the n th-order Chebyshev polynomial of the first kind, valid for $n \geq 3$. Note that $c_2(x) = t_2(x)$ and $c_1(x) = t_1(x)$. Therefore,

$$\begin{aligned} \det \mathbf{C}_n(x) &= c_n(x) \\ &= \begin{cases} U_n\left(\frac{x}{2}\right) & \text{if } n \in \{1, 2\}, \\ 2(-1)^n [T_n(-\frac{x}{2}) - 1] & \text{if } n \geq 3. \end{cases} \end{aligned} \quad (94)$$

Now consider a perturbed version of the circulant matrix above:

$$\mathbf{C}_n(x, a) := \begin{pmatrix} x+a & 1 & & & & & 1 \\ 1 & x & 1 & & & & \\ & 1 & x & 1 & & & \\ & & \ddots & \ddots & \ddots & & \\ & & & 1 & x & 1 & \\ & & & & 1 & x & 1 \\ 1 & & & & & 1 & x \end{pmatrix}. \quad (95)$$

Cofactor evaluation of its determinant gives

$$\det \mathbf{C}_n(x, a) = \det \mathbf{C}_n(x) + a \det \mathbf{T}_{n-1}(x). \quad (96)$$

Specializing to $n \geq 3$ evaluates this to

$$\begin{aligned} \det \mathbf{C}_n(x, a) &= 2(-1)^n \left[T_n\left(-\frac{x}{2}\right) - 1 \right] + a U_{n-1}\left(\frac{x}{2}\right) \\ &= 2(-1)^n \left(1 + \frac{a}{n} \frac{\partial}{\partial x} \right) \left[T_n\left(-\frac{x}{2}\right) - 1 \right]. \end{aligned} \quad (97)$$

Notice that this means

$$\det \mathbf{C}_n(x, a) = \left(1 + \frac{a}{n} \frac{\partial}{\partial x} \right) \det \mathbf{C}_n(x), \quad (98)$$

which can be also be verified using Jacobi's identity. Direct evaluation for $n = 1$ and $n = 2$ show that Eq. (98) is also valid for those cases and therefore valid for all $n \in \mathbb{N}_+$. Equations (91), (94), and (97) are used in Section IV.

-
- [1] “Global surveillance disclosures page on Wikipedia [http://en.wikipedia.org/wiki/Global_surveillance_disclosures_\(2013%E2%80%93present\)](http://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present)); see the references therein for additional details,” Wikipedia page, 2014.
- [2] M. Movahedi, J. Saia, and M. Zamani, “Secure Anonymous Broadcast,” arxiv:1405.5326v1 [cs.DC] (2014).

- [3] F. Stajano and R. Anderson, “The Cocaine Auction Protocol: On the Power of Anonymous Broadcast,” in *Information Hiding* (Springer Berlin Heidelberg, Berlin, Heidelberg, 2000), pp. 434–447.
- [4] D. Chaum, “The dining cryptographers problem: Unconditional sender and recipient untraceability,” *J. Cryptology* 1 (1988).

- [5] A. Broadbent and A. Tapp, “Information-theoretic security without an honest majority,” in *Proceedings of ASIACRYPT 2007*, pp. 410–426 (2007).
- [6] A. Broadbent, S. Jeffrey, and A. Tapp, “Exact, Efficient and Information-Theoretically Secure Voting with an Arbitrary Number of Cheaters,” arXiv:1011.5242 [cs.CR] (2010).
- [7] P. Boykin, *Information security and quantum mechanics: security of quantum protocols*, Ph.D. thesis, University of California, Los Angeles, 2002.
- [8] M. Christandl and S. Wehner, “Quantum Anonymous Transmissions,” in *Proceedings of ASIACRYPT 2005, LNCS 3788* (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005), pp. 217–235.
- [9] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp, “Anonymous quantum communication,” in *Proceedings of ASIACRYPT, 2007*, pp. 460–473 (2007).
- [10] X.-Q. Cai and H.-F. Niu, “Quantum Private Communication with an Anonymous Sender,” *Int. J. Theor. Phys.* **52**, 411 (2013).
- [11] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge, 2000).
- [12] T. F. Demarie, T. Linjordet, N. C. Menicucci, and G. K. Brennen, “Detecting topological entanglement entropy in a lattice of quantum harmonic oscillators,” *New J. Phys.* **16**, 085011 (2014).
- [13] J. K. Pachos, *Introduction to Topological Quantum Computation* (Cambridge University Press, 2012).
- [14] R. Barends *et al.*, “Superconducting quantum circuits at the surface code threshold for fault tolerance,” *Nature* **508**, 500 (2014).
- [15] M. Suchara, J. Kubiatowicz, A. Faruque, F. Chong, C. Lai, and G. Paz-Silva, *Proceedings of the 31st IEEE International Conference on Computer Design* (2013), p. 419.
- [16] A. Y. Kitaev, “Fault-tolerant quantum computation by anyons,” *Annals of Physics* **303**, 2 (2003).
- [17] J. Pachos, *Introduction to Topological Quantum Computation* (Cambridge University Press, 2012).
- [18] A. Hamma, R. Ionicioiu, and P. Zanardi, “Bipartite entanglement and entropic boundary law in lattice spin systems,” *Phys. Rev. A* **71**, 022315 (2005).
- [19] S. S. Bullock and G. K. Brennen, “Qudit surface codes and gauge theory with finite cyclic groups,” *J. Phys. A: Math. Theor.* **40**, 3481 (2007).
- [20] A. G. Fowler, A. C. Whiteside, and L. C. L. Hollenberg, “Towards practical classical processing for the surface code: Timing analysis,” *Phys. Rev. A* **86**, 042313 (2012).
- [21] H. Anwar, *Towards Fault-Tolerant Quantum Computation with Higher-Dimensional Systems*, Ph.D. thesis, University College London, London, 2014.
- [22] G. Brennen, D. Song, and C. Williams, “Quantum-computer architecture using nonlocal interactions,” *Phys. Rev. A* **67**, 050302 (2003).
- [23] J. Zhang, C. Xie, K. Peng, and P. van Loock, “Anyon statistics with continuous variables,” *Phys. Rev. A* **78**, 052121 (2008).
- [24] J. Zhang, “Local complementation rule for continuous-variable four-mode unweighted graph states,” *Phys. Rev. A* **78**, 034301 (2008).
- [25] M. Gagen and G. Milburn, “Atomic tests of the Zeno effect,” *Phys. Rev. A* **47**, 1467 (1993).
- [26] A. Beige and G. Hegerfeldt, “Projection postulate and atomic quantum Zeno effect,” *Phys. Rev. A* **53**, 53 (1996).
- [27] J. M. Dominy, G. A. Paz-Silva, A. T. Rezakhani, and D. Lidar, “Analysis of the quantum Zeno effect for quantum control and computation,” *J. Phys. A: Math. Theor.* **46**, 075306 (2013).
- [28] P. Wang, M. Chen, N. C. Menicucci, and O. Pfister, “Weaving quantum optical frequency combs into continuous-variable hypercubic cluster states,” *Phys. Rev. A* **90**, 032325 (2014).
- [29] M. Chen, N. C. Menicucci, and O. Pfister, “Experimental Realization of Multipartite Entanglement of 60 Modes of a Quantum Optical Frequency Comb,” *Phys. Rev. Lett.* **112**, 120505 (2014).
- [30] N. C. Menicucci, “Temporal-mode continuous-variable cluster states using linear optics,” *Phys. Rev. A* **83**, 062314 (2011).
- [31] S. Yokoyama *et al.*, “Ultra-large-scale continuous-variable cluster states multiplexed in the time domain,” *Nature Photonics* **7**, 982 (2013).
- [32] T. Eberle *et al.*, “Quantum Enhancement of the Zero-Area Sagnac Interferometer Topology for Gravitational Wave Detection,” *Phys. Rev. Lett.* **104**, 251102 (2010).
- [33] M. Mehmet, S. Ast, T. Eberle, S. Steinlechner, H. Vahlbruch, and R. Schnabel, “Squeezed light at 1550 nm with a quantum noise reduction of 12.3 dB,” *Opt. Express* **19**, 25763 (2011).
- [34] G. Paz-Silva, S. Rebić, J. Twamley, and T. Duty, “Perfect Mirror Transport Protocol with Higher Dimensional Quantum Chains,” *Phys. Rev. Lett.* **102**, 020503 (2009).
- [35] B. Yurke *et al.*, “Observation of 4.2-K equilibrium-noise squeezing via a Josephson-parametric amplifier,” *Physical Review Letters* **60**, 764 (1988).
- [36] M. A. Castellanos-Beltran, K. D. Irwin, G. C. Hilton, L. R. Vale, and K. W. Lehnert, “Amplification and squeezing of quantum noise with a tunable Josephson metamaterial,” *Nature Phys.* **4**, 929 (2008).
- [37] E. Flurin, N. Roch, F. Mallet, M. H. Devoret, and B. Huard, “Generating Entangled Microwave Radiation Over Two Transmission Lines,” *Phys. Rev. Lett.* **109**, 183901 (2012).
- [38] N. Bergeal, F. Schackert, L. Frunzio, and M. H. Devoret, “Two-Mode Correlation of Microwave Quantum Noise Generated by Parametric Down-Conversion,” *Phys. Rev. Lett.* **108**, 123902 (2012).
- [39] C. Eichler *et al.*, “Observation of Two-Mode Squeezing in the Microwave Frequency Domain,” *Phys. Rev. Lett.* **107**, 113601 (2011).
- [40] C. M. Wilson *et al.*, “Observation of the dynamical Casimir effect in a superconducting circuit,” *Nature* **479**, 376 (2011).
- [41] M. H. Devoret, S. Girvin, and R. Schoelkopf, “Circuit-QED: How strong can the coupling between a Josephson junction atom and a transmission line resonator be?,” *Annalen der Physik* **16**, 767 (2007).
- [42] S. Ashhab and F. Nori, “Qubit-oscillator systems in the ultrastrong-coupling regime and their potential for preparing nonclassical states,” *Phys. Rev. A* **81**, 042311 (2010).
- [43] M. S. Allman *et al.*, “Tunable Resonant and Nonresonant Interactions between a Phase Qubit and LC Resonator,” *Phys. Rev. Lett.* **112**, 123601 (2014).
- [44] K. Moon and S. Girvin, “Theory of Microwave Parametric Down-Conversion and Squeezing Using Circuit QED,” *Phys. Rev. Lett.* **95**, 140504 (2005).

- [45] A. Zagorin, E. Il'ichev, M. McCutcheon, J. Young, and F. Nori, "Controlled Generation of Squeezed States of Microwave Radiation in a Superconducting Resonant Circuit," *Phys. Rev. Lett.* **101**, 253602 (2008).
- [46] W. Yi Huo and G. Lu Long, "Entanglement and squeezing in solid-state circuits," *New J. Phys.* **10**, 013026 (2008).
- [47] P.-B. Li and F.-L. Li, "Engineering squeezed states of microwave radiation with circuit quantum electrodynamics," *Phys. Rev. A* **83**, 035807 (2011).
- [48] N. C. Menicucci, S. T. Flammia, and P. van Loock, "Graphical calculus for Gaussian pure states," *Phys. Rev. A* **83**, 042335 (2011).
- [49] S. Diehl, A. Micheli, A. Kantian, B. Kraus, H. P. Büchler, and P. Zoller, "Quantum states and phases in driven open quantum systems with cold atoms," *Nature Phys.* **4**, 878 (2008).
- [50] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (John Wiley & Sons, 2012).
- [51] E. T. Jaynes, *Probability Theory, The Logic of Science* (Cambridge University Press, 2003).
- [52] T. Stace, S. Barrett, and A. Doherty, "Thresholds for Topological Codes in the Presence of Loss," *Phys. Rev. Lett.* **102**, 200501 (2009).
- [53] G. Grimmett, *Percolation* (Springer Science & Business Media, 1999).
- [54] N. C. Menicucci, S. T. Flammia, and O. Pfister, "One-Way Quantum Computing in the Optical Frequency Comb," *Phys. Rev. Lett.* **101**, 130501 (2008).
- [55] S. T. Flammia, N. C. Menicucci, and O. Pfister, "The Optical Frequency Comb as a One-Way Quantum Computer," *J. Phys. B* **42**, 114009 (2009).
- [56] R. N. Alexander, S. C. Armstrong, R. Ukai, and N. C. Menicucci, "Noise analysis of single-mode Gaussian operations using continuous-variable cluster states," *Phys. Rev. A* **90**, 062324 (2014).
- [57] J. Borowska and L. Łacińska, "Recurrence form for determinant of a heptadiagonal symmetric Toeplitz matrix," *Journal of Applied Mathematics and ...* (2014).
- [58] Z. Cinkir, "A fast elementary algorithm for computing the determinant of Toeplitz matrices," *Journal of Computational and Applied Mathematics* **255**, 353 (2014).
- [59] G. Y. Hu and R. F. O'Connell, "Analytical inversion of symmetric tridiagonal matrices," *J. Phys. A: Math. Gen.* **29**, 1511 (1996).
- [60] M. Elouafi, "On a relationship between Chebyshev polynomials and Toeplitz determinants," *Applied Mathematics and Computation* **229**, 27 (2014).
- [61] R. Álvarez-Nodarse, J. Petronilho, and N. R. Quintero, "Spectral properties of certain tridiagonal matrices," *Linear Algebra and its Applications* **436**, 682 (2012).
- [62] C. M. Da Fonseca and J. Petronilho, "Explicit inverse of a tridiagonal k-Toeplitz matrix," *Numerische Mathematik* **100**, 457 (2005).
- [63] We have assumed, without loss of generality, that the face and edge orientation at the edge e_A of the intersection of the arc $\mathcal{P}_2(\text{Alice})$ and the loop $\tilde{\mathcal{P}}_2$ satisfies $(-1)^{f(e_A)+o(e_A)} = 1$; otherwise, r acquires that sign.
- [64] If one can additionally squeeze the string mode \hat{f}_2 by a factor s_2 , then the protocol improves with the modified parameters $\epsilon = \frac{w}{2s^4s_2^2}$ and $\alpha = 2s^2s_2^2\tau^2$.
- [65] The variance restriction on the capacity is henceforth understood.
- [66] Rather than engineering the always-on Hamiltonian \hat{H}_{int} , one could instead simulate the interaction via repeated sequences of discrete evolution of the unitary $U(\tau) = e^{-i\hat{H}_{\text{int}}\tau}$ for short times $\tau \sim 1/\delta$ followed by complete decay of the ancillary modes. The unitary $U(\tau)$ is a Gaussian operation and could be decomposed into a gate sequence involving small connected networks of 5 modes, each consisting of single-mode squeezing, phase shifters, and beam splitters. The issue of engineering the interaction across boundaries of wedges would require ancillary modes that are shared between nearest-neighbor parties.